

1
2
3
4
5
6
7 **UNITED STATES DISTRICT COURT**
8 **FOR THE WESTERN DISTRICT OF WASHINGTON**
9 **AT SEATTLE**

10 R.S.,

11 *on behalf of himself and all others*
12 *similarly situated,*

13 Plaintiff,

14 v.

15 COSTCO WHOLESALE
16 CORPORATION.

17 Defendant.

Case No.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

18 1. Plaintiff R.S.,¹ at all times relevant herein, has filled prescriptions and received
19 pharmacy services from Costco Wholesale Corporation (“Costco” or “Defendant”), and brings this
20 class action individually and on behalf of all others similarly situated, and alleges, upon personal
21 knowledge as to his own actions, his counsels’ investigation, and upon information and belief as
22 to all other matters, as follows:

23 2. Plaintiff brings this case to address Defendant’s unlawful practice of disclosing
24 Plaintiff’s and Class Members’ confidential, personally-identifiable information (“PII”) and
25
26

27 ¹ Plaintiff brings this action anonymously out of a desire to protect his personal health information under the Health
28 Insurance Portability and Accountability Act of 1996 and Washington and California law.

1 protected, health information (“PHI”) (collectively referred to as “Private Information”) to
2 unauthorized third parties via tracking technologies and analytics software embedded on its
3 website (“Tracking Tools”). One of the Tracking Tools Defendant installed on its Website is the
4 Facebook pixel, which works in conjunction with related marketing tools and caused patients’
5 Private Information to be sent to Meta Platforms, Inc. d/b/a Meta (“Facebook”) without patients’
6 consent when they used Defendant’s website.
7

8 3. On information and belief, Defendant’s websites and Tracking Tools have also
9 transmitted patients’ Private Information to additional unauthorized third-parties for marketing and
10 advertising purposes, including Google and Adobe.

11 4. Defendant owns and controls <https://www.costco.com/pharmacy> (“Defendant’s
12 Website” or the “Website”), which it encourages its patients to use for the following purposes: (1)
13 to register for the Costco Member Prescription Program (“CMPP”), which allows patients to enter
14 and refill prescriptions directly from the warehouse; (2) enroll in its Rx Mail Order program or
15 view their existing home delivery account; (3) check the status of their prescriptions; (4) find
16 information about their prescription medications, pricing, and insurance coverage for Costco’s
17 Mail Order Pharmacy; and (6) to locate other information related to their prescriptions and medical
18 treatment.
19

20 5. Under the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”),
21 pharmacies such as Defendant’s are “covered entities” and are required to follow strict rules
22 regarding the use and disclosure of individuals’ health information.²
23
24
25

26 ² 42 U.S.C. § 1320d; 45 C.F.R. Part 160-45 C.F.R. Part 162, and 45 C.F.R. Part 164. Defendant is
27 engaged in the sale and dispensing of drugs in accordance with prescriptions, and therefore
28 qualifies as a “person or organization who furnishes, bills, or is paid for health care.” *Id.*

6. Unbeknownst to patients, Defendant installed Tracking Tools on its Website, which surreptitiously manipulated their web browsers, thereby causing their communications with the Defendant via the Website to be shared and/or intercepted by unauthorized third parties.

7. Plaintiff and Class Members used the Website to submit information related to their prescriptions. The Private Information unauthorized third parties received revealed individual patients' identities and details about the confidential health care they sought and received from Defendant, including the name of their prescription medications, dosage, and form of the medication, and more. In turn, these disclosures allow third parties to reasonably infer that a specific patient was being treated for a specific type of medical condition such as cancer, pregnancy, HIV, mental health conditions, and an array of other symptoms or conditions.

8. The information collected and disclosed by Defendant's Tracking Tools is not anonymous. Facebook connects user data from Defendant's Website to the individual's Facebook ID (FID). The FID links the user to his/her Facebook profile, which contains detailed information about the profile owner's identity.

9. Similarly, Google "stores users' logged-in identifier on non-Google website in its logs. Whenever a user logs-in on non-Google websites, whether in private browsing mode or non-private browsing mode, the same identifier is associated with the data Google collects from the user's browsing activities on that website. Google further logs all such data (private and non-private) within the same logs and uses these data for serving personalized ads."³

³ See *Brown v. Google, Inc.*, *Brown v. Google LLC*, 525 F. Supp. 3d 1049 (N.D. Cal. 2021) (citing internal evidence from Google employees). Google also connects user data to IP addresses; IP addresses have been classified by the United States Department of Health and Human Services ("HHS") as personally identifying information. *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, U.S. Dept of Health and Hum. Servs. (Dec. 1, 2022), <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html>.

1 10. Simply put, the health information disclosed through the Tracking Tools is
2 personally identifiable.

3 11. The United States Department of Health and Human Services (HHS) has
4 established “Standards for Privacy of Individually Identifiable Health Information” (also known
5 as the HIPAA “Privacy Rule”) governing how health care providers must safeguard and protect
6 Private Information. Under the Privacy Rule, no health care provider – including pharmacies like
7 Defendant – can disclose a person’s personally identifiable protected health information to a third
8 party without express written authorization.

9
10 12. In addition, as explained further below, HHS has specifically warned healthcare
11 regulated entities—such as Defendant—that tracking technologies like the ones used on its
12 Website transmit personally identifying information to third parties, and that such information
13 should not be transmitted without a HIPAA-compliant written authorization from patients.

14
15 13. The Federal Trade Commission (FTC) has also warned hospitals and other entities
16 that “even if you are not covered by HIPAA, you still have an obligation to protect against
17 impermissible disclosures of personal health information under the FTC Act and the FTC Health
18 Breach Notification Rule.”⁴

19
20
21 ⁴ The FTC further clarified that entities who are not covered by HIPAA are nonetheless required
22 to obtain affirmative express consent prior to disclosing health information, which is defined as:
23 “any freely given, specific, informed, and unambiguous indication of an individual’s wishes
24 demonstrating agreement by the individual, such as by a clear affirmative action, following a
25 Clear and Conspicuous disclosure to the individual, apart from any ‘privacy policy,’ ‘terms of
26 service,’ ‘terms of use,’ or other similar document, of all information material to the provision of
27 consent. Acceptance of a general or broad terms of use or similar document that contains
28 descriptions of agreement by the individual along with other, unrelated information, does not
constitute Affirmative Express Consent. Hovering over, muting, pausing, or closing a given
piece of content does not constitute Affirmative Express Consent. Likewise, agreement obtained
through use of a user interface designed or manipulated with the substantial effect of subverting
or impairing user autonomy, decision-making, or choice, does not constitute Affirmative Express

14. In addition, both Washington and California state law, including the Washington Uniform Health Care Information Act (“WUHCIA”) and California Medical Information Act (“CMIA”) expressly prohibits the disclosure of Private Information without express written authorization.

15. Despite these clear laws and regulations, Defendant has essentially planted a bug on patients’ web browsers that forced them disclose private and confidential communications to third parties. Defendant did not disclose the presence of these Tracking Tools to Website users filling prescriptions with Costco.

16. Patients simply do not anticipate or expect that their trusted healthcare provider will send personal health information or confidential medical information regarding their prescriptions to a hidden third party—let alone social media networks and online advertisers like Facebook, which has a sordid history of privacy violations in pursuit of ever-increasing advertising revenue—without patient consent. Patients did not sign a written authorization permitting Defendant to send their Private Information to Facebook, and Defendant does not have a HIPAA-compliant business associate agreement with Facebook.

17. Defendant breached its statutory and common law obligations to its patients by, inter alia,: (i) failing to remove or disengage technology that was known and designed to share patients Private Information, including sensitive details such as the exact name of their prescription medications; (ii) failing to obtain the written consent of patients to disclose their Private Information to Facebook and any other unauthorized third parties with whom Defendant has failed to execute a HIPAA-compliant business associate agreement; (iii) failing to take steps to block the

Consent.” *United States of America v. Easy Healthcare Corporation d/b/a Easy Healthcare* (N.D. Ill 2023), Stipulated Settlement accessible online https://www.ftc.gov/system/files/ftc_gov/pdf/2023.06.22_easy_healthcare_signed_order_2023.pdf (last access October 13, 2023).

transmission of patients' Private Information via Tracking Tools on its Website; (iv) failing to warn patients; and (v) otherwise failing to design, and monitor its Website to maintain the confidentiality and integrity of patient Private Information.

18. As a result of Defendant's conduct, patients have suffered numerous injuries, including: (i) invasion of privacy; (ii) loss of benefit of the bargain, (iii) diminution of value of the Private Information, (iv) statutory damages, and (v) the continued and ongoing risk to their Private Information.

19. Plaintiff seeks to remedy these harms and brings causes of action for (1) violation of Washington's Consumer Protection Act ("WCPA"), RCW § 19.86.020; (2) violation of Washington's Privacy Act, RCW § 9.73.030; (3) violation of the Electronics Communication Privacy Act ("ECPA") 18 U.S.C. § 2511(1) – unauthorized interception, use, and disclosure; (4) breach of implied contract; (5) breach of fiduciary duty of confidentiality; (6) unjust enrichment; (7) negligence; (8) violation of the California Invasion of Privacy Act ("CIPA"), Cal. Penal Code § 630, *et seq.*; and (9) violations of the California Medical Information Act ("CMIA"), Cal. Civ. Code § 56, *et seq.*.

PARTIES

20. Plaintiff R.S. is a natural person and citizen of California, where he intends to remain, and he is one of Defendant's patients.

21. Defendant, Costco Wholesale Corporation is a Washington general stock corporation with its principal place of business located at 999 Lake Drive, Issaquah, WA 98027.

22. Among other retail services as a "membership warehouse club," Defendant offers one-stop shopping for prescription medications:

Costco members who want the value and quality of our products now have the convenience and privacy of shopping at home. You can order new prescriptions and refills for medications currently

filled at Costco.com, 24 hours a day. They can be delivered anywhere in the United States. Costco.com offers a wide variety of non-prescription remedies, vitamins & herbal supplements, and home health monitors & devices to help you manage your health.⁵

23. Defendant is a covered entity under the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. § 1320d and 45 C.F.R. Part 160-45 C.F.R. Part 162, and 45 C.F.R. Part 164 (“HIPAA”)).

JURISDICTION & VENUE

24. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this case is brought as a class action where the amount in controversy exceeds the sum or value of \$5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different than Defendant.

25. This Court has federal question jurisdiction under 28 U.S.C. § 1331 because this Complaint alleges question of federal laws under the ECPA (18 U.S.C. § 2511, *et seq.*).

26. The Court has personal jurisdiction over Defendant because Costco Wholesale Corporation is headquartered in this District at 999 Lake Drive, Issaquah, WA 98027.

27. Venue is proper under 28 U.S.C § 1391(b)(1) because Defendant’s principal place of business is in this District.

COMMON FACTUAL ALLEGATIONS

A. The U.S. Department of Health and Human Services and Federal Trade Commission Have Warned about Use of Tracking Tools by Healthcare Providers

28. In December 2022, HHS issued a bulletin (the “HHS Bulletin”) warning regulated entities like Defendant about the risks presented by the use of Tracking Tools on their websites:

⁵ <https://www.costco.com/pharmacy/about-home-delivery> (last visited October 12, 2023).

Regulated entities [those to which HIPAA applies] are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules. ***For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures.***⁶

In other words, the HHS has expressly stated that entities who implement Tracking Tools, such as Defendant, have violated HIPAA Rules unless they have obtained a HIPAA-complaint authorization from their patients.

29. The HHS Bulletin further warns that:

While it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors, ***because of the proliferation of tracking technologies collecting sensitive information, now more than ever, it is critical for regulated entities to ensure that they disclose PHI only as expressly permitted or required by the HIPAA Privacy Rule.***⁷

30. In addition, HHS and the FTC have recently issued a letter, once again admonishing entities like Defendant to stop using Tracking Tools:

If you are a covered entity or business associate (“regulated entities”) under HIPAA, you must comply with the HIPAA Privacy, Security, and Breach Notification Rules (HIPAA Rules), with regard to protected health information (PHI) that is transmitted or maintained in electronic or any other form or medium. ***The HIPAA Rules apply when the information that a regulated entity collects through tracking technologies or discloses to third parties (e.g., tracking technology vendors) includes PHI.*** . . . Even if you are not covered by HIPAA, you still have an obligation to protect against impermissible disclosures of personal health information under the FTC Act and the FTC Health Breach Notification Rule. . . . As recent FTC enforcement actions demonstrate, it is essential to monitor data flows of health information to third parties via technologies you have integrated into your website or app. The disclosure of such information without a consumer’s authorization can, in some circumstances, violate the FTC Act as well

⁶ See *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates* (Dec. 1, 2022), available at <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html> (last visited October 11, 2023) (emphasis added).

⁷ *Id.*

as constitute a breach of security under the FTC's Health Breach Notification Rule.⁸

B. Underlying Web Technology

31. To understand Defendant's unlawful data-sharing practices, it is important first to understand basic web design and tracking tools.

32. Devices (such as computer, tablet, or smart phone) access web content through a web browser (e.g., Google's Chrome browser, Mozilla's Firefox browser, Apple's Safari browser, and Microsoft's Edge browser).

33. Every website is hosted by a computer "server" that holds the website's contents and through which the entity in charge of the website exchanges communications with Internet users' client devices via their web browsers.

34. Web communications consist of HTTP or HTTPS Requests and HTTP or HTTPS Responses, and any given browsing session may consist of thousands of individual HTTP Requests and HTTP Responses, along with corresponding cookies:

- **Universal Resource Locator ("URL"):** a web address.
- **HTTP Request:** an electronic communication sent from the client device's browser to the website's server. GET Requests are one of the most common types of HTTP Requests. In addition to specifying a particular URL, GET Requests can also send data to the host server embedded inside the URL, and can include cookies.
- **Cookies:** a small text file that can be used to store information on the client device which can later be communicated to a server or servers. Cookies are sent with HTTP Requests from client devices to the host server. Some cookies are "third-

⁸ *Re: Use of Online Tracking Technologies*, U.S. Dept. of Health & Hum. Servs. and Fed. Trade. Comm'n (July 20, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-OCR-Letter-Third-Party-Trackers-07-20-2023.pdf

party cookies,” which means they can store and communicate data when visiting one website to an entirely different website.

- **HTTP Response:** an electronic communication that is sent as a reply to the client device’s web browser from the host server in response to an HTTP Request. HTTP Responses may consist of a web page, another kind of file, text information, or error codes, among other data.⁹

35. Every website is comprised of Markup and “Source code.” Source code is simply a set of instructions that commands the website visitor’s browser to take certain actions when the web page first loads or when a specified event triggers the code. Source code is essentially the back of the website, and the user does not see what happens in the source code.

36. Source code may also command a web browser to send data transmissions to third parties in the form of HTTP Requests quietly executed in the background without notifying the web browser’s user. Tracking Tools are embedded in the Source Code, which instruct the Website to send a second set transmissions to third parties’ servers.

37. By contrast, the Markup is the façade of the Website and what the user sees.

38. As an example, a patient’s HTTP Request seeks specific information from the Defendant’s Website (e.g., “Fill a Prescription” page), and the HTTP Response provides the requested information in the form of “Markup,” forming the webpage’s content and features.

39. When a patient visits the Website and selects the “Online Pharmacy” button, their web browser automatically sends an HTTP Request to Defendant’s web server, which automatically returns an HTTP Response and loads the Markup for that particular webpage. As

⁹ One browsing session may consist of hundreds or thousands of individual HTTP Requests and HTTP Responses.

depicted in the screenshot below, the user only sees the Markup, not Defendant's Source Code or underlying HTTP Requests and Responses.

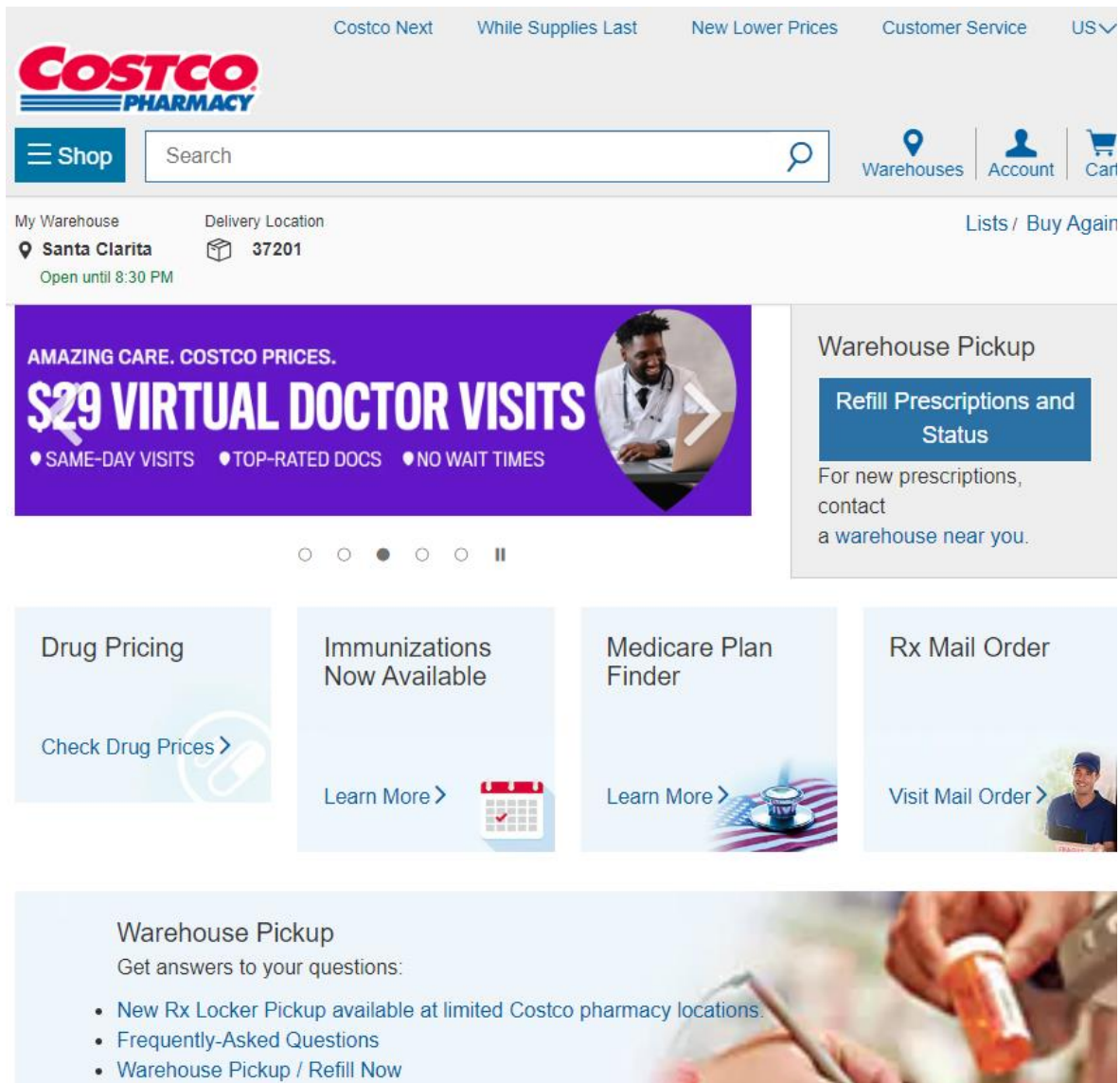


Figure 1. The image above is a screenshot taken from the user's web browser upon visiting www.costco.com/pharmacy (last accessed Oct. 19, 2023).

40. Behind the scenes, Defendant's Tracking Tools effectively open a hidden spying window into the patient's browser, which surreptitiously and automatically records, transmits, and

disseminates, the patients' interactions on the Website, including the exact text they type, the names of their prescription medications, and other Private Information.¹⁰

C. Tracking Tools

41. Third parties, offer "free" or discounted Tracking Tools to advertisers in the form of software that can be integrated into their webpages, mobile applications, and servers, thereby enabling the interception and collection of user communications and activity on those platforms.

42. The Tracking Tools are used to gather, identify, target, and market products and services to individuals. Thus, while "free" to a website owner such as Defendant, the Tracking Tools are actually bartered in exchange for user data. In the absence of these Tracking Tools, Defendant would have needed to spend money on independent computer engineers and HIPAA compliant software that achieves the same result without violating patients' privacy.

43. In general, Tracking Tools are automatically configured to capture certain information, such as when a user visits a particular webpage and that webpage's URL. Advertisers, such as Defendant, can track other user actions and communications and can create their own tracking parameters by customizing the software on their website.

44. When a user accesses a webpage that is hosting Tracking Tools, the user's communications with the host webpage are instantaneously and surreptitiously duplicated and sent to the third party. For example, the Facebook Pixel on Defendant's Website causes the user's web browser to instantaneously duplicate the contents of the communication with the Website (such as

¹⁰ When used in the context of a screen or visual display, a "pixel" is the smallest unit in such a digital display. An image or video on a device's screen can be made up of millions of individual pixels. For example, the Facebook Pixel is a tiny image file that is so small as to be invisible to website users. It is purposefully designed and camouflaged in this manner so that website users remain unaware of it.

1 a request to fill a particular prescription) and send the duplicate from the user’s browser directly
2 to Facebook’s server.

3 45. Notably, transmissions only occur on webpages that contain Tracking Tools.¹¹
4 Thus, patients’ Private Information would not have been disclosed to Facebook or other
5 unauthorized third parties via this technology but for Defendant’s decisions to install the Tracking
6 Tools on its Website, including webpages that transmit PHI.

7 46. Sometimes a particularly tech-savvy user attempts to circumvent browser-based
8 wiretap technology, so a website operator can also transmit data directly to Facebook through the
9 use of first-party cookies and server-to-server transmission. Users cannot detect or prevent
10 transmissions through first-party cookies.

11 47. Conversions API (“CAPI”) is a Facebook tool that functions as a redundant
12 measure (in addition to the Facebook Pixel) to circumvent any ad blockers or other denials of
13 consent by the website user by transmitting information directly from Defendant’s servers to
14 Facebook’s servers.^{12, 13}

15 48. The third parties to whom a website transmits data through Tracking Tools and
16 associated workarounds such as CAPI do not provide any substantive Website content relating to
17 the user’s communications. Instead, these third parties are typically procured to track user data and
18 communications for marketing purposes of the website owner (*i.e.*, to bolster profits).

19 ¹¹ For example, Defendant’s Facebook Pixel has its own unique identifier (represented as
20 id=I707542376568799), which can be used to identify which of Defendant’s webpages contain the
21 Facebook Pixel.

22 ¹² *What is the Facebook Conversions API and how to use it*, Realbot (last updated May 20, 2022),
23 <https://revealbot.com/blog/facebook-conversions-api/> (last visited Jan. 24, 2023).

24 ¹³ “Server events are linked to a dataset ID and are processed like events sent via the Meta Pixel.... This
25 means that server events may be used in measurement, reporting, or optimization in a similar way as other
26 connection channels.”, <https://developers.facebook.com/docs/marketing-api/conversions-api> (last visited
27 October 10, 2023).

1 49. Thus, without any knowledge, authorization, or action by a user, a website owner
2 like Defendant can use its source code to commandeer the user's computing device, causing the
3 device to re-direct contemporaneously and invisibly the users' communications to third parties.

4 **D. Defendant Disclosed its Patients' Private Information to unauthorized Third Parties**
5 **via Tracking Tools on its Website**

6 50. Without its patients' consent, Defendant has effectively used its source code to
7 commandeer and "bug" or "tap" its patients' computing devices, thereby allowing Facebook and
8 other third parties to listen in on and intercept all their communications with Defendant, including
9 Private Information.

10 51. While seeking and using Defendant's services as a pharmacy and trusted healthcare
11 provider, patients communicated their Private Information via the Website in relation to and in
12 order to obtain medical care and treatment from Defendant.

13 52. Based on this relationship alone, patients had a reasonable expectation of privacy
14 when using the Website, and this is further supported by the fact they were not aware that their
15 Private Information would be shared with third parties as it was communicated to Defendant, and
16 Defendant did not disclose this fact.

17 53. Patients never consented, agreed, authorized, or otherwise permitted Defendant to
18 disclose their Private Information to third parties, nor did they intend for anyone other than
19 Defendant to be a party to their communications (many of them highly sensitive and confidential).

20 54. Importantly, the Private Information Defendant's Tracking Tools sent to third
21 parties included personally identifying information that allowed those third parties to connect the
22 Private Information to a specific patient. Information sent to Facebook was sent alongside the
23 patients' Facebook ID (c_user cookie or "FID"), thereby allowing individual patients'
24
25
26
27
28

1 communications with Defendant, and the Private Information contained in those communications,
2 to be linked to their unique Facebook accounts and therefore their identity.¹⁴

3 55. A user's FID is linked to their Facebook profile, which generally contains a wide
4 range of demographics and other information about the user, including location, pictures, personal
5 interests, work history, relationship status, and other details. Because the user's Facebook ID
6 uniquely identifies an individual's Facebook account, Facebook—or any ordinary person—can
7 easily use the Facebook ID to locate, access, and view the user's corresponding Facebook profile
8 quickly and easily.

10 56. Similarly, Google users who are logged-in to their Google accounts also have an
11 identifier that is stored in Google's logs. Google logs a user's browsing activities on non-Google
12 websites and uses this data for serving personalized ads.

14 57. By installing and implementing the Tracking Tools, Defendant caused patients
15 communications to be intercepted by and/or disclosed to Facebook and exploited for marketing.

16 58. As explained below, these unlawful transmissions are initiated by Defendant's
17 source code concurrent with communications made via certain webpages.

18 **E. Defendant's Tracking Tools Disseminate Patient Information Via Its Website**

19 59. The images below illustrate the point. When a patient used the Website to search
20 for his specific prescription medication, "Cabergoline," the Website delivers information including
21 "Pricing" and "Drug Information." Patients are encouraged to communicate additional information
22 via the filters and drop-down tabs in the left menu, including whether they are seeking the brand-
23

26 ¹⁴ Defendant's Website track and transmit data via first-party and third-party cookies. The c_user cookie or
27 FID is a type of third-party cookie assigned to each person who has a Facebook account, and it is comprised
28 by a unique and persistent set of numbers.

name or generic version of the drug, the form (such as tablet or liquid), the dosage and strength of the medication, packing, and quantity.

My Warehouse: Vacaville, Open until 8:30 PM
Delivery Location: 94533
[Lists / Buy Again](#)

Home / Member Prescription Program / Cabergoline

Brand/Generic: Cabergoline...
Form: Tablet
Strength: 0.5 mg
Package: Bottle
Quantity: 8

Prescription Name:
[Get Prices](#)

Cabergoline
(0.5 mg, 8 tablets)
[Pricing](#) [Drug Information](#)

Use your Costco membership number to save on prescription medications!

Find a participating pharmacy
Show membership card & prescription
Receive your Costco member price and save!

COSTCO PHARMACY	\$22.79	View Locations
COSTCO WHOLESALE Prescription Home Delivery	\$24.79	Get Started Online
SAFEWAY	\$30.99	View Locations

Figure 2.

60. Unbeknownst to ordinary patients, this webpage—which is undoubtedly used to communicate Private Information for the purpose of obtaining health care—contained Defendant's Tracking Tools and sent every communication made via the webpage to Facebook. It also logs and transmits instantaneously the patient's location alongside their Private Information.

61. The image below, which is a screenshot taken from a network traffic report, confirms that Facebook received patients' Private Information, including the names of their prescription medications, when patients used the Website.

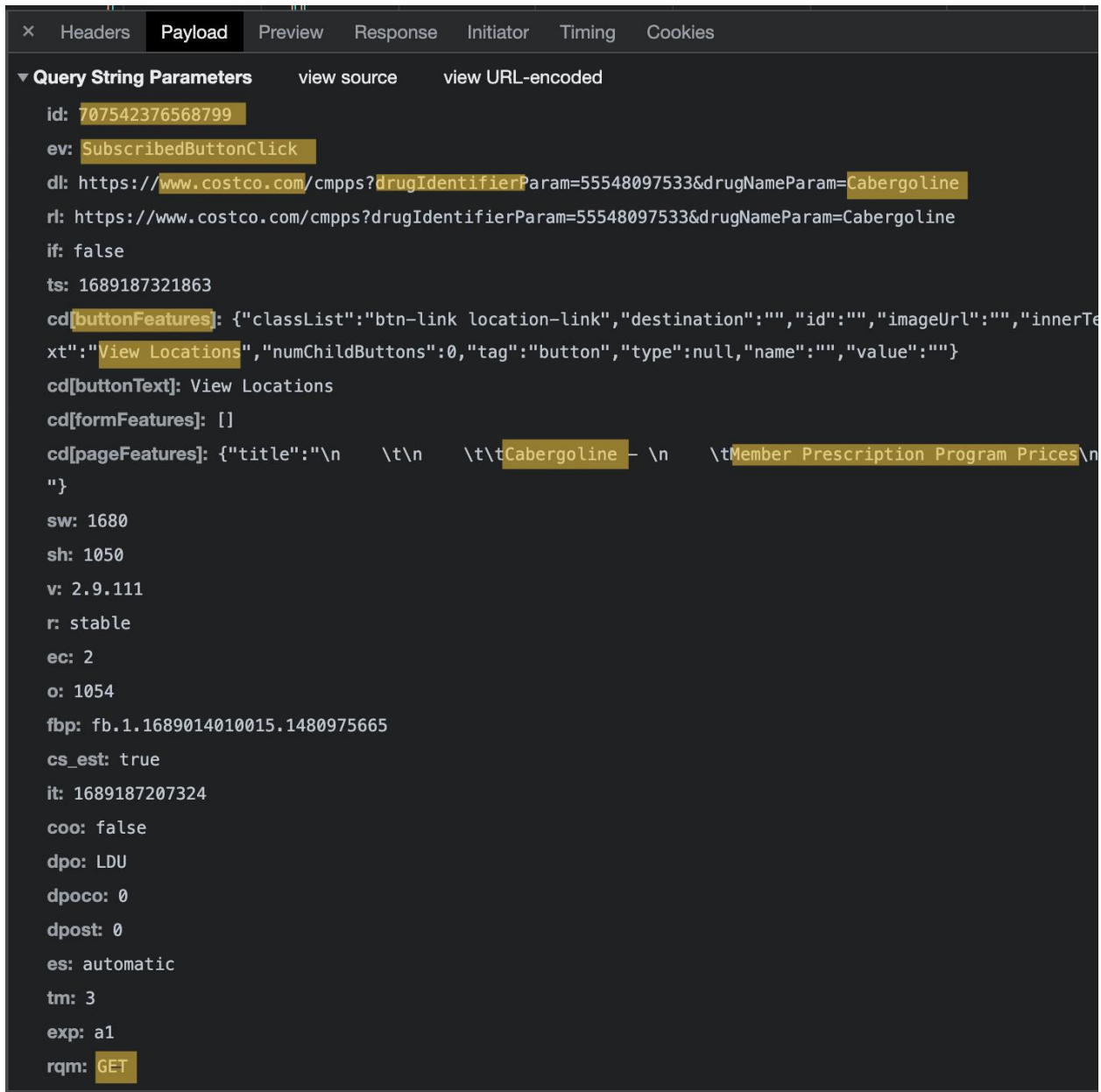


Figure 3.

62. As shown in Figure 3, when the user searched for his specific prescription medication (Cabergoline) via the Website, Facebook received that exact phrase.

63. The first line of highlighted text, “id: 707542376568799” refers to Defendant’s Pixel ID and confirms that it installed the Facebook Pixel into its Source Code on this webpage.

1 64. The second line of text, “ev: SubscribedButtonClick,” identifies and categorizes
2 which actions the user took on the Webpage (“ev:” is an abbreviation for event, and
3 “SubscribedButtonClick” is the type of event). Thus, this identifies the user as having searched for
4 the specific drug, “Cabergoline.”

5 65. The additional lines of highlighted text show Defendants disclosed to Facebook:
6 (1) the fact that the user is seeking a particular prescription; (2) using search parameters for drug
7 comparison pricing; (3) selecting the least expensive option through the Costco Member
8 Prescription Program (“CMPP”), and (4) that they searched for specific locations close to them in
9 order to acquire the particular medication.
10

11 66. Finally, the highlighted text (“GET”) demonstrates that Defendant’s Pixel sent the
12 user’s communications, and the Private Information contained therein, alongside the user’s
13 Facebook ID (c_user ID), thereby allowing the user’s communications and actions on the website
14 to be linked to their specific Facebook profile.
15
16
17
18
19
20
21
22
23
24
25
26
27
28

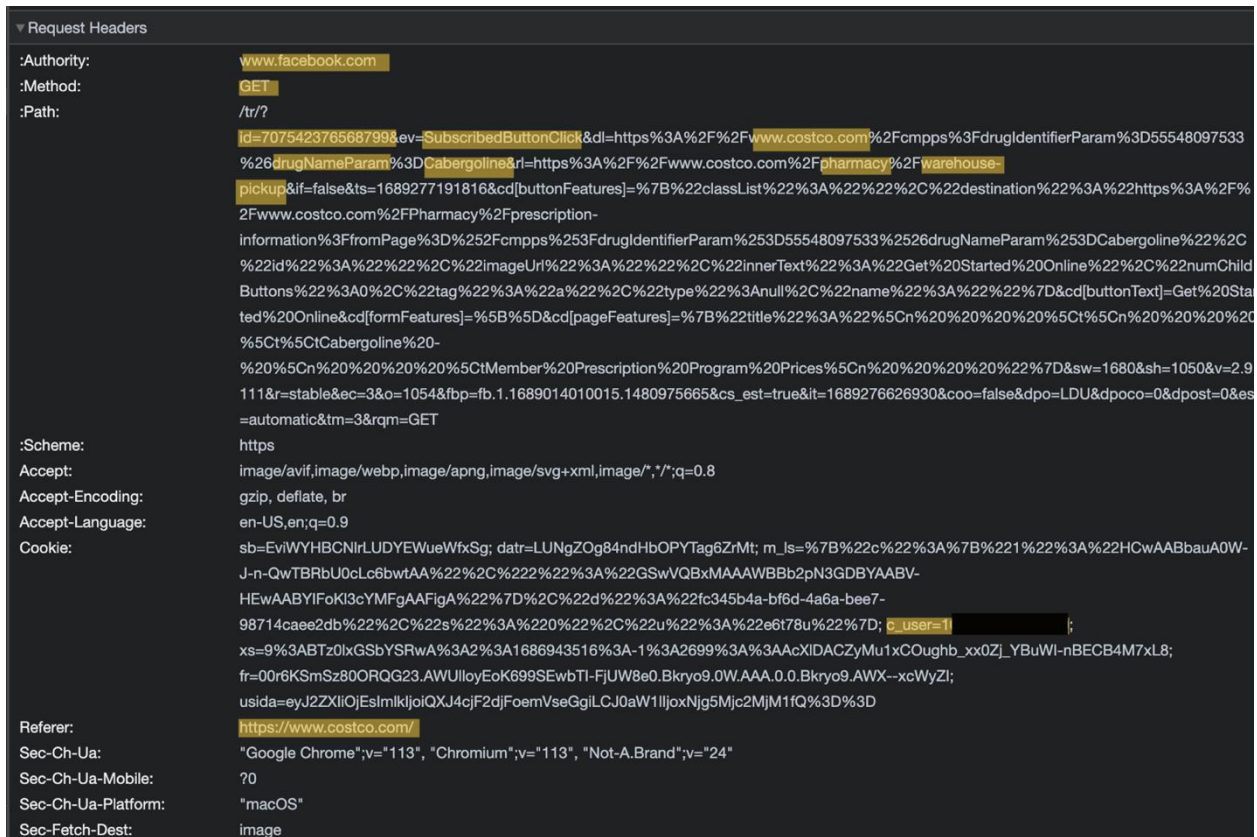


Figure 4. Screenshot of the user's network traffic depicting the user's URL Request headers associated with Defendant's Pixel ID 707542376568799.

67. The image demonstrates that the user’s Facebook ID (highlighted as “c_user=” in the image above) was sent alongside the other data.¹⁵

68. Defendant's pixel also tracks and records instances in which a user searches amongst various Medicare plans that the Defendant will accept to pay for Medicare Part D prescriptions. The user must visit a separate site, but the Defendant's pixel tracks the buttons the user selects to go to the next site and transmits that information to Facebook as exemplified below:



Figure 5. Screenshot take from the user's traffic report depicting the "Payload" and corresponding "Headers" associated with the user's online activity and communications to Defendant.

¹⁵ The user's Facebook ID is represented as the c_user ID highlight in the image below, and Plaintiff has redacted the corresponding string of numbers to preserve the user's anonymity.

1 69. As with the previous example, the user's search parameters and filters are
2 communicated to Facebook via Defendant's pixel, and their search for Medicare plans is recorded
3 as a "SubscribedButtonClick" alongside the site they are taken to providing them with the best
4 Costco Preferred Plans.¹⁶

5
6 70. In each of the examples above, the user's website activity and the contents of the
7 user's communications are sent to Facebook alongside their personally identifiable information in
8 the form of their FID.

9
10 71. At present, the full breadth of Defendant's tracking and data sharing practices is
11 unclear, but other evidence suggests Defendant is using additional Tracking Tools to transmit its
12 patients' Private Information to additional third parties.

13 **F. Plaintiff R.S.'s Experience**

14 72. Plaintiff is a patient who has received Defendant's pharmaceutical services on
15 several occasions, and he used the Website to communicate his Private Information to Defendant
16 in relation to and in order to obtain pharmaceutical services from Defendant.

17 73. Plaintiff has been a Facebook user since at least 2008.

18
19 74. Plaintiff accessed and used the Website to communicate his Private Information at
20 Defendant's direction and with its encouragement, and he specifically recalls using the Website to
21 communicate sensitive information concerning his prescription medications.

22 75. As a result of using the Website in this manner, and pursuant to the systematic
23 process described in this Complaint, unauthorized third parties received Plaintiff's Private
24 Information, including the medical information he submitted via the Website.

25
26
27 ¹⁶ In addition to protecting information about health conditions, HIPAA also covers health care plans and
28 protects information regarding the payment of medical bills. 45 C.F.R. §164.501.

1 76. Defendant intercepted or assisted these interceptions without Plaintiff's knowledge,
 2 consent, or express written authorization. By failing to receive the requisite consent, Defendant
 3 breached confidentiality and unlawfully disclosed Plaintiff's Private Information.

4 77. As Defendant's patient, Plaintiff reasonably expected that his online
 5 communications with Defendant were solely between him and Defendant and that these
 6 communications would not be transmitted to or disclosed to a third party. But for his status as
 7 Defendant's patient, Plaintiff would not have disclosed his Private Information to Defendant.
 8

9 78. During his time as a patient, Plaintiff never consented to the use of his Private
 10 Information by third parties or to Defendant enabling third parties, including Facebook, to access
 11 or interpret such information.

12 79. During the same transmissions, the Tracking Tools routinely provide third parties
 13 with patients' FIDs, IP addresses, and/or device IDs or other information they input into
 14 Defendant's Website, like their home address, zip code, or phone number. This is precisely the
 15 type of information that HIPAA requires healthcare providers to anonymize to protect the privacy
 16 of patients.
 17

18 80. After intercepting and collecting this information, Facebook processes it, analyzes
 19 it, and assimilates it into datasets like Core Audiences and Custom Audiences. If the Website
 20 visitor is also a Facebook user, Facebook will associate the information that it collects from the
 21 visitor with a Facebook ID that identifies their name and Facebook profile, i.e., their real-world
 22 identity. A user's Facebook Profile ID is linked to their Facebook profile, which generally contains
 23 a wide range of demographics and other information about the user, including pictures, personal
 24 interests, work history, relationship status, and other details. Because the user's Facebook Profile
 25 ID uniquely identifies an individual's Facebook account, Meta—or any ordinary person—can
 26
 27
 28

1 easily use the Facebook Profile ID to locate, access, and view quickly and easily the user's
2 corresponding Facebook profile.

3 81. Upon information and belief, as a “redundant” measure to ensure patients Private
4 Information was successfully transmitted to unauthorized third parties and exploited for marketing
5 purposes, Defendant implemented server-based workarounds like Conversions API, which
6 transmit Private Information from electronic storage on Defendant’s server directly to Meta’s
7 server; i.e. the Private Information was transmitted regardless of patients’ browser settings.
8

9 82. Patients suffered injuries in the form of (i) invasion of privacy; (ii) diminution of
10 value of their Private Information; (iii) statutory damages; (iv) the continued and ongoing risk to
11 their Private Information; and (v) the continued and ongoing risk of harassment, spam, and targeted
12 advertisements specific to their medical conditions and other confidential information
13 communicated to Defendant via the Website.
14

15 83. Plaintiff has a continuing interest in ensuring that future communications with
16 Defendant are protected and safeguarded from future unauthorized disclosure.

17 **G. Defendant’s Conduct Is Unlawful and Violated Industry Norms**

18 ***i. Defendant Violated HIPAA Standards***

19 84. Under Federal Law, a healthcare provider may not disclose personally identifiable,
20 non-public medical information about a patient, a potential patient, or household member of a
21 patient for marketing purposes without the patients’ express written authorization.¹⁷
22

23 85. The HIPAA Privacy Rule, located at 45 CFR Part 160 and Subparts A and E of Part
24 164, “establishes national standards to protect individuals’ medical records and other individually
25 identifiable health information (collectively defined as ‘protected health information’) and applies
26

27 ¹⁷ HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502; 164.508(a)(3), 164.514(b)(2)(i).
28

1 to health plans, health care clearinghouses, and those health care providers that conduct certain
2 health care transactions electronically.”¹⁸

3 86. The Privacy Rule broadly defines “protected health information” (“PHI”) as
4 individually identifiable health information (“IIHI”) that is “transmitted by electronic media;
5 maintained in electronic media; or transmitted or maintained in any other form or medium.” 45
6 C.F.R. § 160.103.

7
8 87. IIHI is defined as “a subset of health information, including demographic
9 information collected from an individual” that is: (1) “created or received by a health care provider,
10 health plan, employer, or health care clearinghouse”; (2) “[r]elates to the past, present, or future
11 physical or mental health or condition of an individual; the provision of health care to an
12 individual; or the past, present, or future payment for the provision of health care to an individual”;
13 and (3) either (a) “identifies the individual” or (b) “[w]ith respect to which there is a reasonable
14 basis to believe the information can be used to identify the individual.” 45 C.F.R. § 160.103.

15
16 88. Under the HIPPA de-identification rule, “health information is not individually
17 identifiable only if”: (1) an expert “determines that the risk is very small that the information could
18 be used, alone or in combination with other reasonably available information, by an anticipated
19 recipient to identify an individual who is a subject of the information” and “documents the methods
20 and results of the analysis that justify such determination”; or (2) “the following identifiers of the
21 individual or of relatives, employers, or household members of the individual are removed;
22

23 a. Names;

24 ***

25 H. Medical record numbers;

26
27 ¹⁸ HHS.gov, HIPAA For Professionals (last visited October 12, 2023),
28 <https://www.hhs.gov/hipaa/forprofessionals/privacy/index.html>.

J. Account numbers;

M. Device identifiers and serial numbers;

N. Web Universal Resource Locators (URLs);

O. Internet Protocol (IP) address numbers; ... and

R. Any other unique identifying number, characteristic, or code...;and”

The covered entity must not “have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.”

45 C.F.R. § 160.514.

89. The HIPAA Privacy Rule requires any “covered entity”—which includes pharmacies—to maintain appropriate safeguards to protect the privacy of protected health information and sets limits and conditions on the uses and disclosures that may be made of protected health information without authorization. 45 C.F.R. §§ 160.103, 164.502.

90. An individual or corporation violates the HIPAA Privacy Rule if it knowingly and in violation of 42 U.S.C. §§ 1320d-1320d-9 (“Part C”): “(1) uses or causes to be used a unique health identifier; [or] (2) obtains individually identifiable health information relating to an individual.” The statute states that a “person ... shall be considered to have obtained or disclosed individually identifiable health information in violation of [Part C] if the information is maintained by a covered entity ... and the individual obtained or disclosed such information without authorization.” 42 U.S.C. § 1320d-6.

91. The criminal and civil penalties imposed by 42 U.S.C. § 1320d-6 apply directly to Defendant when it is knowingly disclosing individually identifiable health information relating to an individual, as those terms are defined under HIPAA.

92. Violation of 42 U.S.C. § 1320d-6 is subject to criminal penalties. 42 U.S.C. § 1320d-6(b). There is a penalty enhancement where “the offense is committed with intent to sell,

transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm.” In such cases, the entity that knowingly obtains individually identifiable health information relating to an individual shall “be fined not more than \$250,000, imprisoned not more than 10 years, or both.”

93. In Guidance regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act Privacy Rule, the HHS instructs:

Identifying information alone, such as personal names, residential addresses, or phone numbers, would not necessarily be designated as PHI. For instance, if such information was reported as part of a publicly accessible data source, such as a phone book, then this information would not be PHI because it is not related to health data... If such information was listed with health condition, health care provision, or payment data, such as an indication that the individual was treated at a certain clinic, then this information would be PHI.¹⁹

94. In its guidance for Marketing, the HHS further instructs:

The HIPAA Privacy Rule gives individuals important controls over whether and how their protected health information is used and disclosed for marketing purposes. With limited exceptions, the Rule requires an individual’s written authorization before a use or disclosure of his or her protected health information can be made for marketing. ... Simply put, a covered entity may not sell protected health information to a business associate or any other third party for that party’s own purposes. Moreover, *covered entities may not sell lists of patients to third parties without obtaining authorization from each person on the list.* (Emphasis added).²⁰

95. As alleged above, there is an HHS Bulletin that highlights the obligations of “regulated entities,” which are HIPAA-covered entities and business associates, when using tracking technologies.²¹

¹⁹https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf (last visited October 11, 2023).

²⁰<https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/marketing.pdf> (last visited Oct. 12, 2023)

²¹ See <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html>.

1 96. The Bulletin expressly provides that “[r]egulated entities are not permitted to use
2 tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking
3 technology vendors or any other violations of the HIPAA Rules.”

4 97. Defendant’s actions violated HIPAA Rules.

5 **H. Patients’ Expectation of Privacy**

6 98. Plaintiff and Class Members were aware of Defendant’s duty of confidentiality
7 when they sought medical services from Defendant.

8 99. Indeed, at all times when patients provided their Private Information to Defendant,
9 they had a reasonable expectation that the information would remain private and that Defendant
10 would not share the Private Information with third parties for a commercial purpose (such as
11 marketing), unrelated to patient care.

12 100. Plaintiff and Class Members would not have used the Website, would not have
13 provided their Private Information to Defendant, and would not have paid for Defendant’s
14 healthcare services, or would have paid less for them, had they known that Defendant would
15 disclose their Private Information to third parties.

16 **I. IP Addresses Are PII**

17 101. Defendant also disclosed and otherwise assisted third parties with intercepting
18 patients’ device IP addresses.

19 102. An IP address is a unique number that identifies the address of a particular device
20 connected to the Internet, which is used to identify and route communications on the Internet.

21 103. IP addresses of individual Internet users are used by Internet service providers,
22 websites, and third-party tracking companies to facilitate and track Internet communications.

23 104. For example, Facebook tracks every IP address ever associated with a Facebook
24 user, and it uses that information to target individual homes and their occupants with advertising.
25
26
27
28

105. Under HIPAA, an IP address is considered PII:

- HIPAA defines PII to include “any unique identifying number, characteristic or code” and specifically lists the example of IP addresses. *See* 45 C.F.R. § 164.514 (2).
- HIPAA further declares information as personally identifiable where the covered entity has “actual knowledge that the information to identify an individual who is a subject of the information.” 45 C.F.R. § 164.514(2)(ii); *See* also, 45 C.F.R. § 164.514(b)(2)(i)(O).

106. Consequently, by disclosing IP addresses, Defendant’s business practices violated HIPAA and industry privacy standards.

J. Defendant Was Enriched and Benefitted from the Use of The Tracking Tools and Unauthorized Disclosures

107. The primary motivation and a determining factor in Defendant’s interception and disclosure of Plaintiff’s and Class Members’ Private Information was to commit criminal and tortious acts in violation of federal and state laws as alleged herein, namely, the use of patient data for advertising in the absence of express written consent. Defendant’s further use of the Private Information after the initial interception and disclosure for marketing and revenue generation was in violation of HIPAA and an invasion of privacy. In exchange for disclosing the Private Information of its patients, Defendant is compensated in the form of enhanced advertising services and more cost-efficient marketing on its platform.

108. Retargeting is a form of online marketing that targets users with ads based on their previous internet communications and interactions.

109. Upon information and belief, as part of its marketing campaign, Defendant re-targeted patients and potential patients to get more patients to use its services. Defendant did so

1 through use of the intercepted patient data it obtained, procured, and/or disclosed in the absence
2 of express written consent.

3 110. By utilizing the Tracking Tools, the cost of advertising and retargeting was reduced
4 through further use of the unlawfully intercepted and disclosed Private Information, thereby
5 benefitting Defendant while invading the privacy of Plaintiff and Class Members and violating
6 their rights under federal and California law.
7

8 **K. Patients' Private Information Had Financial Value**

9 111. Patients' Private Information has economic value. Facebook regularly uses data
10 that it acquires to create Core and Custom Audiences, as well as Lookalike Audiences and then
11 sells that information to advertising clients. Google has recognized the value of user data and has
12 even instituted a pilot program in which it pays users \$3 per week to track them online.
13

14 112. Data harvesting is one of the fastest growing industries in the country, and
15 consumer data is so valuable that it has been described as the "new oil." Conservative estimates
16 suggest that in 2018, Internet companies earned \$202 per American user from mining and selling
17 data. That figure is only due to continuing to increase; estimates for 2022 are as high as \$434 per
18 user, for a total of more than \$200 billion industry wide.

19 113. The value of health data in particular is well-known and has been reported on
20 extensively in the media. For example, Time Magazine published an article in 2017 titled "How
21 Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry" in which it described the
22 extensive market for health data and observed that the market for information was both lucrative
23 and a significant risk to privacy.²²
24
25
26

27 ²² See <https://time.com/4588104/medical-data-industry/> (last visited October 10, 2023).
28

1 114. Similarly, CNBC published an article in 2019 in which it observed that “[d]e-
 2 identified patient data has become its own small economy: There’s a whole market of brokers who
 3 compile the data from providers and other health-care organizations and sell it to buyers.”²³

4 **TOLLING**

5 115. Any applicable statute of limitations has been tolled by the “delayed discovery”
 6 rule. Plaintiff did not know (and had no way of knowing) that his Private Information was
 7 intercepted and unlawfully disclosed to third parties because Defendant kept this information
 8 secret, and the Tracking Tools were invisible.

9 **CLASS ACTION ALLEGATIONS**

10 116. Plaintiff brings this action on behalf of himself and all other persons similarly
 11 situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

12 117. The Nationwide Class that Plaintiff seeks to represent is defined as follows:

13 All individuals residing in the United States who are, or were, patients of Defendant
 14 or any of its affiliates, who used Defendant’s Website and had their Private
 15 Information disclosed to a third party without authorization or consent.

16 In the alternative, Plaintiff seeks to represent a California Subclass defined as:

17 All individuals residing in California who are, or were, patients of Defendant or
 18 any of its affiliates, used Defendant’s Website, and had their Private Information
 19 disclosed to a third party without authorization or consent.

20 The Nationwide Class and California Class are collectively referred to as the “Class.”

21 118. Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries,
 22 any entity in which Defendant has a controlling interest, any of Defendant’s officers or directors,
 23 any successor or assign, and any Judge who adjudicates this case, including their staff and
 24 immediate family members.

25
 26
 27 ²³ See <https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html> (last visited October 10, 2023).

1 119. Plaintiff reserves the right to modify or amend the definition of the proposed class
2 before the Court determines whether certification is appropriate.

3 120. Numerosity, Fed R. Civ. P. 23(a)(1). The Class Members are so numerous that the
4 membership of all members is impracticable. Upon information and belief, there are hundreds of
5 thousands of individuals whose Private Information was improperly disclosed to third parties as a
6 result of Defendant's use of the Tracking Tools on its Website, and the Class is identifiable within
7 Defendant's records.
8

9 121. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3). Questions of law and fact
10 common to the Class exist and predominate over any questions affecting only individual Class
11 Members. These include:

12 a. Whether and to what extent Defendant had a duty to protect the Private Information
13 of Plaintiff and Class Members;
14

15 b. Whether Defendant had duties not to disclose the Private Information of Plaintiff
16 and Class Members to unauthorized third parties;

17 c. Whether Defendant adequately, promptly, and accurately informed Plaintiff and
18 Class Members that their Private Information would be disclosed to third parties;

19 d. Whether Defendant violated the law by failing to notify promptly Plaintiff and
20 Class Members that their Private Information had been compromised;
21

22 e. Whether Defendant adequately addressed and fixed the practices which permitted
23 the disclosure of patient Private Information;

24 f. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing
25 to safeguard the Private Information of Plaintiff and Class Members;
26
27
28

g. Whether Defendant’s conduct violated the Washington Consumer Protection Act RCW § 19.86.020;

h. Whether Defendant’s conduct violated the California Invasion of Privacy Act (“CIPA”), Cal. Penal Code § 630, *et seq.*;

i. Whether Defendant’s conduct violated the California Medical Information Act (“CMIA”), Cal. Civ. Code § 56, *et seq.*;

j. Whether Defendant’s conduct violated the California Unfair Competition Law (“UCL”), Cal. Bus. & Prof. Code § 17200, *et seq.*;

k. Whether Plaintiff and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant’s wrongful conduct; and

l. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and ongoing harm faced as a result of Defendant’s disclosure of their Private Information.

122. Typicality, Fed. R. Civ. P. 23(a)(3). Plaintiff’s claims are typical of those of other Class Members because all had their Private Information compromised as a result of Defendant’s incorporation of Tracking Tools, due to Defendant’s misfeasance.

123. Adequacy, Fed. R. Civ. P. 23(a)(4). Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that Plaintiff has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages Plaintiff has suffered are typical of other Class Members. Plaintiff has also retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

124. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3). Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against a large corporation like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

125. Policies Generally Applicable to the Class. Fed. R. Civ. P. 23(b)(2). This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

126. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources;

1 the costs of individual suits could unreasonably consume the amounts that would be recovered;
2 proof of a common course of conduct to which Plaintiff was exposed is representative of that
3 experienced by the Class and will establish the right of each Class Member to recover on the cause
4 of action alleged; and individual actions would create a risk of inconsistent results and would be
5 unnecessary and duplicative of this litigation.
6

7 127. The litigation of the claims is manageable. Defendant's uniform conduct, the
8 consistent provisions of the relevant laws, and the ascertainable identities of Class Members
9 demonstrate that there would be no significant manageability problems with prosecuting this
10 lawsuit as a class action.

11 128. Adequate notice can be given to Class Members directly using information
12 maintained in Defendant's records.
13

14 129. Unless a class-wide injunction is issued, Defendant may continue disclosing the
15 Private Information of Class Members, Defendant may continue to refuse to provide proper
16 notification to Class Members regarding the practices complained of herein, and Defendant may
17 continue to act unlawfully as set forth in this Complaint.

18 130. Further, Defendant has acted or refused to act on grounds generally applicable to
19 the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the
20 Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil
21 Procedure.
22

23 131. Issue Certification, Fed. R. Civ. P. 23(c)(4). Likewise, particular issues are
24 appropriate for certification because such claims present only particular, common issues, the
25 resolution of which would advance the disposition of this matter and the parties' interests therein.
26 Such particular issues include, but are not limited to, the following:
27
28

1 a. Whether Defendant owed a legal duty to not disclose Plaintiff's and Class
2 Members' Private Information;

3 b. Whether Defendant breached a legal duty to Plaintiff and Class Members to
4 exercise due care in collecting, storing, using, and safeguarding their Private Information;

5 c. Whether Defendant failed to comply with its own policies and applicable laws,
6 regulations, and industry standards relating to data security;

7 d. Whether Defendant adequately and accurately informed Plaintiff and Class
8 Members that their Private Information would be disclosed to third parties;

9 e. Whether Defendant failed to implement and maintain reasonable security
10 procedures and practices appropriate to the nature and scope of the information disclosed to third
11 parties;

12 f. Whether Class Members are entitled to actual, consequential, and/or nominal
13 damages, and/or injunctive relief as a result of Defendant's wrongful conduct.
14
15
16

17 **COUNT I**
18 **VIOLATIONS OF THE WASHINGTON CONSUMER PROTECTION ACT**
19 **RCW § 19.86.020**
20 **(On behalf of Plaintiff and the Class)**

21 132. Plaintiff incorporates the prior allegations as if fully set forth herein and brings this
22 Count individually and on behalf of the proposed Class.

23 133. This cause of action is brought pursuant to the Washington Consumer Protection
24 Act ("WCPA"), RCW §19.86.020, which protects consumers from "Unfair methods of
25 competition and unfair or deceptive acts or practices in the conduct of any trade or commerce...."
26
27
28

1 134. By reason of the conduct alleged herein, Defendant engaged in unlawful practices
2 within the meaning of WCPA § 19.86.020 . The conduct alleged herein is a “business practice”
3 within the meaning of WCPA § 19.86.020, and the deception occurred within Washington State.

4 135. By serving as Plaintiff’s and Class Members’ healthcare provider through their
5 pharmacy, Defendant had a duty to protect Plaintiff’s and Class Members’ Private Information
6 from unlawful disclosure.

7 136. Plaintiff and the Class Members paid for or otherwise availed themselves and
8 received services from Defendant, for the purpose of filling prescriptions and receiving pharmacy
9 services.

10 137. Defendant engaged in the conduct alleged herein, entering into transactions
11 intended to result, and which did result, in the provision of health care treatment and pharmacy
12 services to Plaintiff and Class Members.

13 138. Defendant’s acts, practices, and omissions were done in the course of offering
14 health care treatment, services, and care throughout the state of Washington and the United States.

15 139. The unfair and deceptive acts and practices of Defendant alleged herein, and in
16 particular the decisions regarding the Tracking Tools, emanated and arose within the state of
17 Washington, within the scope of WCPA § 19.86.020.

18 140. Defendant, operating in and out of Washington, engaged in unfair and deceptive
19 trade acts or practices in the conduct of trade or commerce, in violation of WCPA § 19.86.020,
20 including but not limited to the following: (a) knowingly promising to protect Plaintiff’s and Class
21 Members’ Private Information, (b) knowingly and improperly storing, possessing, using, and/or
22 procuring the interception of, Plaintiff’s and Class Members’ Private Information; and
23 (c) knowingly disclosing Plaintiff’s and Class Members’ Private Information to third parties.
24
25
26
27
28

1 141. Defendant committed these acts while concurrently representing that it would
2 protect and not unlawfully disclose Plaintiff's and Class Members' Private Information unless
3 under a legal obligation to do so.

4 142. These unfair and deceptive acts and practices violated duties imposed by laws,
5 including by not limited to HIPAA, the Washington Privacy Act, the Washington Cybercrime Act,
6 the Washington Uniform Health Care Information Act, statutes regarding the confidentiality of
7 medical records, and WCPA § 19.86.020.

8 143. Defendant knew or should have known that its Website and the Tracking Tools
9 thereon was unlawfully wiretapping, intercepting, and disclosing Plaintiff's and Class Members'
10 Private Information.

11 144. Defendant's unfair conduct and business practices affect the public interest. As
12 described herein, a person's medical information, including prescription drug information, is
13 protected by HIPAA and Washington and California state law. The public has the right to control
14 the dissemination and disclosure of private health information and not have its trust violated by
15 the surreptitious interception and disclosure of that information.

16 145. Plaintiff has standing to pursue this claim because as a direct and proximate result
17 of Defendant's violations of WCPA § 19.86.020, Plaintiff and Class Members have been injured
18 by a violation of WCPA § 19.86.020 and bring this action to obtain a declaratory judgment that
19 Defendant's acts or practices violate WCPA § 19.86.020.

20 146. Plaintiff also has standing to pursue this claim because, as a direct result of
21 Defendant's knowing violation of WCPA § 19.86.020, Plaintiff and Class Members have lost
22 money or property in the form monies paid for Defendant's services, diminution in value of their
23 Private Information, as well as loss of the benefit of their bargain with Defendant.

1 147. Plaintiff and Class Members are entitled to injunctive relief to protect them from
2 the substantial and imminent risk of future loss of Private Information, including, but not limited
3 to: (a) ordering that Defendant immediately remove any pixel, web beacon, cookie, or other
4 tracking technology that causes the disclosure of Private Information to third parties without
5 consent; (b) ordering that Defendant engage third-party security auditors and internal personnel to
6 ensure Plaintiff's and Class Members' Private Information is no longer subject to the unlawful
7 practices described in this Complaint; (c) ordering that Defendant purge, delete, and destroy
8 Private Information not necessary for its provisions of services in a reasonably secure manner;
9 (d) ordering that Defendant routinely and continually conduct internal training and education to
10 inform internal security personnel how to properly handle Private Information provided via
11 Defendant's Website; (e) ordering Defendant to meaningfully educate individuals about the threats
12 they face as a result of the loss of their Private Information to third parties, as well as the steps
13 victims should take to protect themselves.
14

15
16 148. Plaintiff brings this action individually and on behalf of Class Members for the
17 relief requested above and for the public benefit in order to promote the public interests in the
18 provision of truthful, fair information to allow consumers to make informed purchasing decisions
19 and to protect Plaintiff, Class Members, and the public from Defendant's unfair methods of
20 competition and unfair, unconscionable, and unlawful practices. Defendant's wrongful conduct as
21 alleged in this Class Action Complaint has had a widespread impact on the public at large.
22

23 149. The above unfair, unconscionable, and unlawful practices and acts by Defendant
24 were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to
25 Plaintiff and Class Members that they could not reasonably avoid; this substantial injury
26 outweighed any benefits to consumers or to competition.
27
28

150. Defendant's actions and inactions in engaging in the unfair and deceptive practices described herein were negligent, knowing and willful, or wanton and reckless.

151. Plaintiff and Class Members seek relief under WCPA § 19.86.020, including, but not limited to, a declaratory judgment that Defendant's actions and/or practices violate WCPA § 19.86.020; injunctive relief enjoining Defendant, their employees, parents, subsidiaries, affiliates, executives, and agents from continuing to violate WCPA § 19.86.020 as described above.

152. Plaintiff and Class Members are also entitled to recover treble actual damages, to recover the costs of this action (including reasonable attorneys' fees), and such other relief as the Court deems just and proper.

COUNT II
VIOLATIONS OF THE WASHINGTON PRIVACY ACT ("WPA")
RCW § 9.73.030, et seq.
(On Behalf of Plaintiff and the Class)

153. Plaintiff incorporates the prior allegations as if fully set forth herein and brings this Count individually and on behalf of the proposed Class.

154. The Washington Privacy Act ("WPA") makes it "unlawful for any individual, partnership, corporation, association, or the state of Washington, its agencies, and political subdivisions to intercept or record any private communications transmitted by telephone, telegraph, radio, or other device between two or more individuals between points within or without the state by any device electronic or otherwise designed to record and/or transmit said communication regardless how such device is powered or actuated, without first obtaining the consent of all the participants in the communication." RCW § 9.73.030 (1)(a).

155. Consent under the WPA is only considered obtained where "one party has announced to all other parties engaged in the communication or conversation, in any reasonably

1 effective manner, that such communication or conversation is about to be recorded or transmitted.”
2 RCW § 9.73.030(3).

3 156. Specifically, Defendant transmitted Plaintiff’s and Class Members’ names and FID
4 to third parties like Facebook for targeted advertising and other commercial purposes, as described
5 herein.

6
7 157. Defendant’s use of Plaintiff’s and Class Members’ names and Private Information
8 did not serve any public interest.

9 158. The unlawful tracking of Plaintiff and Class Members, and disclosure of their
10 names in connection with their Private Information, has caused Plaintiff and Class Members to
11 suffer damages. This includes damage to the value of their information, which Defendant
12 appropriated for its own enrichment. Plaintiff and Class Members have also suffered nominal and
13 actual damages as previously alleged.

14
15 159. Defendant failed to protect Plaintiff’s and Class Members’ Private Information and
16 acted knowingly when it installed the Pixel onto its Website because the purpose of the Pixel is to
17 track and disseminate individual’s communications with the Website for the purpose of marketing
18 and advertising.

19 160. Because Defendant intentionally and willfully incorporated Tracking Tools into its
20 Website and encouraged patients to use that Website for healthcare purposes, Defendant had notice
21 and knew that its practices would cause injury to Plaintiff and Class Members.

22
23 161. Plaintiff, individually and on behalf of Class Members, seeks compensatory
24 damages for Defendant’s invasion of privacy, which includes the value of the privacy interest
25 invaded by Defendant, loss of time and opportunity costs, plus prejudgment interest, and costs.
26 Alternatively, Plaintiff and Class Members are entitled to nominal damages for their injuries.
27
28

1 162. Plaintiff and Class Members are entitled to exemplary statutory damages because of
2 Defendant's knowing violations of their statutory rights to privacy.

3 163. Defendant's wrongful conduct will continue to cause great and irreparable injury
4 to Plaintiff and the Class since their Private Information is still maintained by Defendant and still
5 in the possession of Facebook and other third parties and the wrongful disclosure of the
6 information cannot be undone.

7
8 164. Plaintiff and Class Members have no adequate remedy at law for the injuries
9 relating to Defendant's continued possession of their sensitive and confidential records. A
10 judgment for monetary damages will not undo Defendant's disclosure of the information to
11 Facebook who on information and belief continues to possess and utilize that information.

12 165. Plaintiff, on behalf of herself and Class Members, further seeks injunctive relief to
13 enjoin Defendant from further intruding into Plaintiff's and Class Members' statutory privacy
14 interests.
15

16 **COUNT III**
17 **VIOLATIONS OF ELECTRONIC COMMUNICATIONS PRIVACY ACT ("ECPA")**
18 **18 U.S.C. § 2511(1) *et seq.***
19 **UNAUTHORIZED INTERCEPTION, USE, AND DISCLOSURE**
20 **(On Behalf of Plaintiff and the Class)**

21 166. Plaintiff incorporates the prior allegations as if fully set forth herein and brings this
22 Count individually and on behalf of the proposed Class.

23 167. The ECPA protects both sending and receipt of communications.

24 168. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire or
25 electronic communications are intercepted, disclosed, or intentionally used in violation of Chapter
26 119.

27 169. The transmissions of Plaintiff's Private Information to Defendant via Defendant's
28 Website qualifies as a "communication" under the ECPA's definition in 18 U.S.C. § 2510(12).

170. The transmissions of Plaintiff's Private Information to medical professionals qualifies as a "communication" under the ECPA's definition in 18 U.S.C. § 2510(2).

171. **Electronic Communications.** The transmission of Private Information between Plaintiff and Class Members and Defendant via its Website with which they chose to exchange communications are "transfer[s] of signs, signals, writing,...data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photo optical system that affects interstate commerce" and are therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(2).

172. **Content.** The ECPA defines content, when used with respect to electronic communications, to "include[] any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8) (emphasis added).

173. **Interception.** The ECPA defines the interception as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device" and "contents ... include any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(4), (8).

174. **Electronic, Mechanical, or Other Device.** The ECPA defines "electronic, mechanical, or other device" as "any device ... which can be used to intercept a[n] ... electronic communication[.]" 18 U.S.C. § 2510(5). The following constitute "devices" within the meaning of 18 U.S.C. § 2510(5):

- a. Plaintiff's and Class Members' browsers;
- b. Plaintiff's and Class Members' computing devices;
- c. Defendant's web servers; and
- d. The Tracking Tools deployed by Defendant to effectuate the sending and acquisition of patient communications

1 175. Whenever Plaintiff and Class Members interacted with Defendant's Website,
2 Defendant, through the Tracking Tools embedded and operating on its Website,
3 contemporaneously and intentionally disclosed, and endeavored to disclose the contents of
4 Plaintiff's and Class Members' electronic communications to third parties without authorization
5 or consent, and knowing or having reason to know that the electronic communications were
6 obtained in violation of the ECPA. 18 U.S.C. § 2511(1)(c).
7

8 176. Whenever Plaintiff and Class Members interacted with Defendant's Website,
9 Defendant, through the Tracking Tools embedded and operating on its Website,
10 contemporaneously and intentionally used, and endeavored to use the contents of Plaintiff's and
11 Class Members' electronic communications, for purposes other than providing health care services
12 to Plaintiff and Class Members without authorization or consent, and knowing or having reason to
13 know that the electronic communications were obtained in violation of the ECPA. 18 U.S.C.
14 § 2511(1)(d).
15

16 177. Whenever Plaintiff and Class Members interacted with Defendant's Website,
17 Defendant, through the Tracking Tools it embedded and operated on its Website,
18 contemporaneously and intentionally redirected the contents of Plaintiff's and Class Members'
19 electronic communications while those communications were in transmission, to persons or
20 entities other than an addressee or intended recipient of such communication.
21

22 178. Defendant's intercepted communications include, but are not limited to, the
23 contents of communications to/from Plaintiff's and Class Members' regarding PII and PHI,
24 treatment, medication, and scheduling.

25 179. By intentionally disclosing or endeavoring to disclose the electronic
26 communications of Plaintiff and Class Members to affiliates and other third parties, while knowing
27
28

1 or having reason to know that the information was obtained through the interception of an
2 electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C.
3 § 2511(1)(c).

4 180. By intentionally using, or endeavoring to use, the contents of the electronic
5 communications of Plaintiff and Class Members, while knowing or having reason to know that the
6 information was obtained through the interception of an electronic communication in violation of
7 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(d).

8 181. Defendant intentionally used the wire or electronic communications to increase its
9 profit margins. Defendant specifically used the Tracking Tools to track and utilize Plaintiff's and
10 Class Members' PII and PHI for financial gain.

11 182. Defendant was not acting under color of law to intercept Plaintiff's and Class
12 Members' wire or electronic communication.

13 183. Patients did not authorize Defendant to acquire the content of their communications
14 for purposes of invading their privacy and exploiting their Private Information for marketing
15 purposes via the Tracking Tools.

16 184. Any purported consent that Defendant received from Plaintiff and Class Members
17 was not valid.

18 185. **Unauthorized Purpose.** Defendant intentionally intercepted the contents of
19 Plaintiff's and Class Members' electronic communications for the purpose of committing a
20 tortious or criminal act in violation of the Constitution or laws of the United States or of any State
21 – namely, violations of HIPAA, the WCPA, the UHCIA, CIPA, CMIA, UCL, and invasion of
22 privacy, among others.
23
24
25
26
27
28

1 186. The ECPA provides that a “party to the communication” may be liable where a
 2 “communication is intercepted for the purpose of committing any criminal or tortious act in
 3 violation of the Constitution or laws of the United States or of any State.” 18 U.S.C § 2511(2)(d).

4 187. Defendant is a “party to the communication” with respect to patient
 5 communications. However, Defendant’s simultaneous, unknown duplication, forwarding, and
 6 interception of Plaintiff’s and Class Members’ Private Information does not qualify for the party
 7 exemption.
 8

9 188. Defendant’s acquisition of patient communications that were used and disclosed to
 10 unauthorized third parties was done for purposes of committing criminal and tortious acts in
 11 violation of the laws of the United States and Washington, including.

- 12 a. Criminal violation of HIPAA, 42 U.S.C. § 1320d-6;
- 13 b. Violation of Washington’s Cybercrime Act, RCW § 9A.90;
- 14 c. Violation of Washington’s Consumer Protection Act (“WCPA”), RCW §
 15 19.86.020;
- 16 d. Violation of Washington’s Uniform Health Care Information Act (“UHCIA”),
 17 RCW § 70.02.020;
- 18 e. Violation of Washington’s Privacy Act, RCW § 9.73.030;
- 19 f. Violation of the California Invasion of Privacy Act, Cal. Penal Code § 630, *et*
 20 *seq.*;
- 21 g. Violation of the California Medical Information Act, Cal. Civ. Code § 56, *et*
 22 *seq.*; and
- 23 h. Violation of the California Unfair Competition Law, Cal. Bus. and Prof. Code
 24 § 17200 *et seq.*
- 25
- 26
- 27
- 28

1 189. Under 42 U.S.C. § 1320d-6, it is a criminal violation for a person to “use[] or
2 cause[] to be used a unique health identifier” or to “disclose[] individually identifiable health
3 information to another person ... without authorization” from the patient.

4 190. The penalty for violation is enhanced where “the offense is committed with intent
5 to sell, transfer, or use individually identifiable health information for commercial advantage,
6 personal gain, or malicious harm.” 42 U.S.C. § 1320d-6.

7 191. Defendant’s conduct violated 42 U.S.C. § 1320d-6 in that it:

- 8 a. Used and caused to be used cookie identifiers associated with specific patients
9 without patient authorization; and
10 b. Disclosed individually identifiable health information to unauthorized third parties
11 without patient authorization.
12

13 192. Defendant’s conduct would be subject to the enhanced provisions of 42 U.S.C.
14 § 1320d-6 because Defendant’s use of Tracking Tools was for Defendant’s commercial advantage
15 to increase revenue from existing patients and gain new patients.
16

17 193. The Tracking Tools, which constitute programs, commanded Plaintiff’s and Class
18 Members’ computing devices to remove and redirect their data and the content of their
19 communications with Defendant to unauthorized third parties.
20

21 194. Defendant knew or had reason to know that the Tracking Tools would command
22 Plaintiff’s and Class Members’ computing devices to remove and redirect their data and the
23 content of their communications with Defendant to unauthorized third parties.

24 195. Defendant is not exempt from ECPA liability under 18 U.S.C. § 2511(2)(d) on the
25 ground that it was a participant in Plaintiff’s and Class Members’ communications via the Website,
26 and that’s because Defendant used its participation in the communications to improperly share
27
28

1 Plaintiff's and Class Members' Private Information with third-parties that did not participate in
2 these communications (such as Facebook), that Plaintiff and Class Members did not know were
3 receiving their individually-identifiable patient health information, and that Plaintiff and Class
4 Members did not consent to receive this information.

5
6 196. Defendant accessed, obtained, and disclosed Plaintiff's and Class Members'
7 Private Information for the purpose of committing the crimes and torts described herein because it
8 would not have been able to obtain the information or the marketing services if it had complied
9 with the law.

10 197. As such, Defendants cannot viably claim any exception to ECPA liability.

11 198. Plaintiff and Class Members have suffered damages as a direct and proximate result
12 of Defendant's invasion of privacy in that:

- 13
14 a. Learning that Defendant has intruded upon, intercepted, transmitted, shared, and used
15 their individually identifiable patient health information (including information about
16 their medical symptoms, conditions, and concerns, medical appointments, healthcare
17 providers and locations, medications and treatments, and health insurance and
18 medical bills) for commercial purposes has caused Plaintiff and the Class Members
19 to suffer emotional distress;
- 20
21 b. Defendant received substantial financial benefits from its use of Plaintiff's and Class
22 Members' individually identifiable patient health information without providing any
23 value or benefit to Plaintiff or the Class Members;
- 24
25 c. Defendant received substantial, quantifiable value from its use of Plaintiff's and Class
26 Members' individually identifiable patient health information, such as understanding
27 how people use its website and determining what ads people see on its website,
28

without providing any value or benefit to Plaintiffs or the Class Members;

d. Defendant has failed to provide Plaintiff and the Class Members with the full value of the medical services for which they paid, which included a duty to maintain the confidentiality of their patient information; and

e. The diminution in value of Plaintiffs' and Class Members' PII and PHI and the loss of privacy due to Defendant making sensitive and confidential information, such as patient status, test results, and appointments that Plaintiffs and Class Members intended to remain private no longer private.

199. As a result of Defendant's violation of the ECPA, Plaintiff and Class Members entitled to all damages available under 18 U.S.C. § 2520, including statutory damages of whichever is the greater of \$100 a day for each day of violation or \$10,000, equitable or declaratory relief, compensatory and punitive damages, and attorney's fees and costs.

COUNT IV
BREACH OF IMPLIED CONTRACT
(on behalf of Plaintiff and the Class)

200. Plaintiff incorporates the prior allegations as if fully set forth herein and brings this Count individually and on behalf of the proposed Class.

201. As a condition of utilizing Defendant's Website and receiving services from Defendant's healthcare facilities and professionals, Plaintiff and the Class Members provided their Private Information and compensation for their medical care.

202. When Plaintiff and Class Members provided their Private Information to Defendant, they entered into an implied contract pursuant to which Defendant agreed to safeguard and not disclose their Private Information without consent.

204. Plaintiff and Class Members would not have retained Defendant to provide healthcare services in the absence of an implied contract between them and Defendant obligating Defendant to not disclose Private Information without consent.

205. Defendant breached these implied contracts by disclosing Plaintiff's and Class Members' Private Information without consent to unauthorized third parties.

206. As a direct and proximate result of Defendant's breaches of these implied contracts, Plaintiff and Class Members sustained damages as alleged herein, including but not limited to the loss of the benefit of their bargain and diminution in value of Private Information.

207. Plaintiff and Class Members are entitled to compensatory and consequential damages as a result of Defendant's breach of implied contract.

208. Plaintiff incorporates all prior allegations as if fully set forth herein and brings this Count individually and on behalf of the proposed Class.

209. Medical providers have a duty to their patients to keep non-public medical information completely confidential, and to safeguard sensitive personal and medical information. This duty arises from the implied covenant of trust and confidence that is inherent in the physician-patient relationship.

1 210. Plaintiff and Class Members had reasonable expectations of privacy in their
2 communications exchanged with Defendant, including communications exchanged on
3 Defendant's Website.

4 211. In light of the special relationship between Defendant and Plaintiff and Class
5 Members, whereby Defendant became a guardian of Plaintiff's and Class Members' Private
6 Information, Defendant became a fiduciary by its undertaking and guardianship of the Private
7 Information, to act primarily for the benefit of its patients, including Plaintiff and Class Members:
8 (1) for the safeguarding of Plaintiff's and Class Members' Private Information; (2) to notify timely
9 Plaintiff and Class Members of disclosure of their Private Information to unauthorized third
10 parties; and (3) to maintain complete and accurate records of what patient information (and where)
11 Defendant did and does store and disclose.
12

13 212. Contrary to its duties as a medical provider and its express and implied promises of
14 confidentiality, Defendant installed its Tracking Tools to disclose and transmit to third parties
15 Plaintiff's and Class Members' communications with Defendant, including Private Information
16 and the contents of such information.
17

18 213. These disclosures were made for commercial purposes without Plaintiff's or Class
19 Members' knowledge, consent, or authorization, and were unprivileged.
20

21 214. The unauthorized disclosures of Plaintiff's and Class Members' Private
22 Information were intentionally caused by Defendant's employees acting within the scope of their
23 employment. Alternatively, the disclosures of Plaintiff's and Class Members' Private Information
24 occurred because of Defendant's negligent hiring or supervision of its employees, its failure to
25 establish adequate policies and procedures to safeguard the confidentiality of patient information,
26
27
28

1 or its failure to train its employees to properly discharge their duties under those policies and
2 procedures.

3 215. The third-party recipients included, but may not be limited to, Facebook. Such
4 information was received by these third parties in a manner that allowed them to identify the
5 Plaintiff and the individual Class Members.
6

7 216. Defendant's breach of the common law implied covenant of trust and confidence is
8 evidenced by its failure to comply with federal and state privacy regulations, including:

- 9 a. By failing to ensure the confidentiality and integrity of electronic PHI Defendant
10 created, received, maintained, and transmitted, in violation of 45 C.F.R. §
11 164.306(a)(1);
- 12 b. By failing to protect against any reasonably anticipated uses or disclosures of
13 electronic PHI that are not permitted under the privacy rules regarding individually
14 identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);
- 15 c. By failing to ensure compliance with the HIPAA security standard rules by its
16 workforce in violation of 45 C.F.R. § 164.306(a)(4);
- 17 d. By failing to obtain satisfactory assurances, including in writing, that its business
18 associates and/or subcontractors would appropriately safeguard Plaintiff's and Class
19 Members PHI;
- 20 e. By failing to implement technical policies and procedures for electronic information
21 systems that maintain electronic PHI to allow access only to those persons or software
22 programs that have been granted access rights in violation of 45 C.F.R. §
23 164.312(a)(1);
- 24 f. By failing to implement technical security measures to guard against unauthorized
25 access to electronic protected health information that is being transmitted over an
26 electronic communications network in violation of 45 C.F.R. § 164.312(e)(1);
- 27 g. By impermissibly and improperly using and disclosing PHI that is and remains
28 accessible to unauthorized persons in violation of 45 C.F.R. § 164.502, et seq.;
- h. By failing to effectively train all members of its workforce (including independent
contractors) on the policies and procedures with respect to PHI as necessary and
appropriate for the members of its workforce to carry out their functions and to
maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. §
164.308(a)(5);

- i. By failing to keep Private Information confidential as required by N.Y. C.P.L.R. 4504;
- j. By failing to keep Private Information confidential as required by N.Y. Pub. Health Law § 2803(3)(f); and
- k. By otherwise failing to safeguard Plaintiff's and Class Members' Private Information.

217. The harm arising from a breach of provider-patient confidentiality includes mental suffering due to the exposure of private information and erosion of the essential confidential relationship between the healthcare provider and the patient.

218. As a direct and proximate cause of Defendant's unauthorized disclosures of patient personally identifiable, non-public medical information, and communications, Plaintiff and Class members were damaged by Defendant's breach in that:

- a. Sensitive and confidential information that Plaintiff and Class members intended to remain private is no longer private;
- b. Plaintiff and Class members face ongoing harassment and embarrassment in the form of unwanted targeted advertisements;
- c. Defendant eroded the essential confidential nature of the provider-patient relationship;
- d. General damages for invasion of their rights in an amount to be determined by a jury;
- e. Nominal damages for each independent violation;
- f. Defendant took something of value from Plaintiff and Class Members and derived benefit therefrom without Plaintiff's and Class Members' knowledge or informed consent and without compensation for such data;
- g. Plaintiff and Class Members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality;
- h. Defendant's actions diminished the value of Plaintiff's and Class Members' Private Information; and
- i. Defendant's actions violated the property rights Plaintiff and Class members have in their Private Information.

COUNT VI
UNJUST ENRICHMENT
(On behalf of Plaintiff and the Class)

219. Plaintiff incorporates the prior allegations as if fully set forth herein and brings this Count individually and on behalf of the proposed Class.

220. Defendant benefits from the use of Plaintiff's and Class Members' Private Information and unjustly retained those benefits at their expense.

221. Plaintiff and Class Members conferred a benefit upon Defendant in the form of Private Information that Defendant collected from Plaintiff and Class Members, without authorization and proper compensation to exceed the limited authorization and access to that information which was given to Defendant.

222. Defendant exceeded any authorization given and instead consciously disclosed and used this information for its own gain, providing Defendant with economic, intangible, and other benefits, including substantial monetary compensation.

223. Defendant unjustly retained those benefits at the expense of Plaintiff and Class Members because Defendant's conduct damaged Plaintiff and Class Members, all without providing any commensurate compensation to Plaintiff and Class Members.

224. The benefit that Defendant derived from Plaintiff and Class Members was not offered by Plaintiff and Class Members gratuitously and rightly belongs to Plaintiff and Class Members. It would be against equity and good conscience for Defendant to be permitted to retain any of the profit or other benefits wrongly derived from the unfair and unconscionable methods, acts, and trade practices alleged in this Complaint.

1 225. Defendant should be compelled to disgorge into a common fund for the benefit of
2 Plaintiff and Class Members all unlawful or inequitable proceeds that Defendant received, and
3 such other relief as the Court may deem just and proper.

4 **COUNT VII**
5 **NEGLIGENCE**
6 **(On behalf of Plaintiff and the Class)**

7 226. Plaintiff incorporates the prior allegations as if fully set forth herein and brings this
8 Count individually and on behalf of the proposed Class.

9 227. Defendant owed Plaintiff and Class Members a duty to keep their Private
10 Information completely confidential, and to safeguard sensitive personal and medical information.

11 228. Plaintiff and Class Members had reasonable expectations of privacy in their
12 communications exchanged with Defendant, including communications exchanged on
13 Defendant's Website.

14 229. Contrary to its duties as a medical provider and its express promises of
15 confidentiality, Defendant installed its Tracking Tools to disclose and transmit to third parties
16 Plaintiff's and Class Members' communications with Defendant, including Private Information
17 and the contents of such information.

18 230. These disclosures were made without Plaintiff's or Class Members' knowledge,
19 consent, or authorization, and were unprivileged.

20 231. The third-party recipients included, but may not be limited to, Facebook.

21 232. As a direct and proximate cause of Defendant's unauthorized disclosures of patient
22 personally identifiable, non-public medical information, and communications, Plaintiff and Class
23 members were damaged by Defendant's breach in that:

- 24 a. Sensitive and confidential information that Plaintiff and Class members intended
25 to remain private is no longer private;

- b. Plaintiff and Class members face ongoing harassment and embarrassment in the form of unwanted targeted advertisements;
- c. Defendant eroded the essential confidential nature of the provider-patient relationship;
- d. General damages for invasion of their rights in an amount to be determined by a jury;
- e. Nominal damages for each independent violation;
- f. Defendant took something of value from Plaintiff and Class Members and derived benefit therefrom without Plaintiff's and Class Members' knowledge or informed consent and without compensation for such data;
- g. Plaintiff and Class Members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality;
- h. Defendant's actions diminished the value of Plaintiff's and Class Members' Private Information; and
- i. Defendant's actions violated the property rights Plaintiff and Class Members have in their Private Information.

COUNT VIII
VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT ("CIPA")
Cal. Penal Code § 630, *et seq*
(on behalf of Plaintiff and the California Class)

233. Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein and brings this count individually and on behalf of the proposed California Class.

234. The California Invasion of Privacy Act ("CIPA") is codified at Cal. Penal Code §§ 630 to 638. The Act begins with its statement of purpose.

The Legislature hereby declares that advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society.

Cal. Penal Code § 630.

235. California Penal Code § 631(a) provides, in pertinent part (emphasis added):

Any person who, by means of any machine, instrument, or contrivance, or in any other manner ... willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or **who aids, agrees with, employs, or conspires** with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, is punishable by a fine not exceeding two thousand five hundred dollars (\$2,500).

236. Under CIPA, a defendant must show it had the consent of all parties to a communication.

237. At all relevant times, Defendant aided, employed, agreed with, and conspired with unauthorized third parties to track and intercept Plaintiff's and Class Members' communications made via the Website. These communications were transmitted to and intercepted by a third party during the communications and without the knowledge, authorization, or consent of Plaintiff and Class Members.

238. Defendant intentionally inserted an electronic listening device onto Plaintiff's and Class Members' web browsers that, without the knowledge and consent of Plaintiff and Class Members, tracked and transmitted the substance of their confidential communications with Defendants to a third party.

239. Defendant willingly facilitated third parties' interception and collection of Plaintiff's and Class Members' private medical information by embedding the Tracking Tools on its Website. Moreover, unlike past Facebook business tools such as the Facebook Like Button and older web beacons, Defendant has full control over the Pixel, including which webpages contain

1 the pixel, what information is tracked and transmitted via the Pixel, and how events are categorized
2 prior to their transmission.

3 240. Defendant's Tracking Tools constitute "machine[s], instrument[s], or
4 contrivance[s]" under the CIPA, and even if they do not, these tools fall under the broad catch-all
5 category of "any other manner."
6

7 241. Defendant failed to disclose its use of the Tracking Tools to specifically track and
8 automatically and simultaneously transmit Plaintiff's and Class Members' communications with
9 Defendant to undisclosed third parties.

10 242. The Private Information that Defendant transmitted via the Tracking Tools, such as
11 specific prescriptions, as well as names, IP addresses, home addresses, FIDs, or other identifying
12 information, constitutes information about Plaintiff's and Class Members' past, present, or future
13 health or health care and therefore constitutes protected health information.
14

15 243. The Tracking Tools are designed such that they transmit each of the actions users
16 take on the Website to a third party alongside and contemporaneously with the user initiating the
17 communication. Thus, the communication is intercepted in transit to the intended recipient,
18 Defendant, and before it reaches Defendant's server.

19 244. As demonstrated above, Defendant violated CIPA by aiding and permitting third
20 parties to intercept and receive its patients' online communications in real time through its
21 Website. These interceptions occurred without Plaintiff's and Class Members' consent, and
22 unauthorized third parties (including but not limited to Facebook) would not have received the
23 contents of these communications but for Defendant's actions and use of the Tracking Tools.
24

25 245. By disclosing Plaintiff's and Class Members' Private Information, Defendant
26 violated Plaintiff's and Class Members' statutorily protected right to privacy.
27
28

246. As a result of the above violations and pursuant to CIPA Section 637.2, Defendant is liable to Plaintiff and Class Members for treble actual damages related to their loss of privacy in an amount to be determined at trial or for statutory damages in the amount of \$5,000 per violation. Section 637.2 specifically states that “[it] is not a necessary prerequisite to an action pursuant to this section that the plaintiffs has suffered, or be threatened with, actual damages.”

247. Under the statute, Defendant also is liable for reasonable attorney’s fees, litigation costs, injunctive and declaratory relief, and punitive damages in an amount to be determined by a jury, but sufficient to prevent the same or similar conduct by the Defendant in the future.

COUNT IX
VIOLATION OF THE CALIFORNIA CONFIDENTIALITY OF MEDICAL
INFORMATION ACT (“CMIA”)
Cal. Civ. Code § 56, et seq
(on behalf of Plaintiff and the California Class)

248. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein and brings this claim individually and on behalf of the proposed California Class.

249. The California Confidentiality of Medical Information Act, Cal. Civ. Code § 56, et seq (“CMIA”) prohibits health care providers from disclosing medical information relating to their patients without a patient’s authorization. Medical information refers to “any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care... regarding a patient’s medical history, mental or physical condition, or treatment.” ‘Individually Identifiable’ means that the medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual...” Cal. Civ. Code § 56.05.

250. Defendant is a healthcare provider as defined by Cal. Civ. Code § 56.06.

1 251. Plaintiff and Class Members are patients of Defendant and, as a health care
2 provider, Defendant has an ongoing obligation to comply with the CMIA's requirements with
3 respect to Plaintiff's and Class Members' confidential medical information.

4 252. As set forth above, names, addresses, telephone numbers, email addresses, device
5 identifiers, web URLs, IP addresses, and/or other characteristics that can uniquely identify specific
6 patients are transmitted to unauthorized third parties in combination with patient prescription drug
7 information and queries. This protected health information and personally identifiable information
8 constitutes confidential information under the CMIA.

9
10 253. Pursuant to the CMIA, the information communicated to Defendants and disclosed
11 to third parties constitutes medical information because it is patient information derived from a
12 health care provider regarding patients' medical treatment and physical condition and is received
13 by third parties in combination with individually identifying information. Cal. Civ. Code
14 § 56.05(i).

15
16 254. As set forth above, Facebook views, processes, and analyzes the confidential
17 medical information it receives via the Facebook Tracking Pixel, conversions API, SDKs, and
18 other Facebook business tools. It then uses the viewed confidential information to create
19 Audiences for advertising and marketing purposes.

20 255. Defendant failed to obtain Plaintiff's and Class Members' authorization for their
21 disclosure of medical information.

22
23 256. Pursuant to CMIA Section 56.11, a valid authorization for disclosure of medical
24 information must: (1) be "clearly separate from any other language present on the same page and
25 ... executed by a signature which serves no other purpose than to execute the authorization;" (2) be
26 signed and dated by the patient or their representative; (3) state the name and function of the third
27
28

1 party that receives the information; and (4) state a specific date after which the authorization
 2 expires. The information set forth on Defendant's Website, including the Website Privacy Policy
 3 and Notice of Privacy Practices, does not qualify as a valid authorization.

4 257. Defendant thus violated the CMIA by disclosing its patients' medical information
 5 to third parties along with the patients' individually identifying information.

6 258. Plaintiff and Class Members seek nominal damages, compensatory damages,
 7 punitive damages, attorneys' fees, and costs of litigation for Defendant's violations of the CMIA.

8 **PRAYER FOR RELIEF**

9 **WHEREFORE**, Plaintiff, on behalf of herself and Class Members, requests judgment
 10 against Defendant and that the Court grant the following:

- 11 A. For an Order certifying the Class and appointing Plaintiff and Counsel to represent
- 12 such Class;
- 13 B. For equitable relief enjoining Defendant from engaging in the wrongful conduct
- 14 alleged in this Complaint pertaining to the misuse and/or disclosure of the Private
- 15 Information of Plaintiff and Class Members;
- 16 C. For injunctive relief requested by Plaintiff, including, but not limited to, injunctive
- 17 and other equitable relief as is necessary to protect the interests of Plaintiff and
- 18 Class Members:
- 19 D. For an award of damages, including, but not limited to, actual, consequential,
- 20 statutory, punitive, and nominal damages, as allowed by law in an amount to be
- 21 determined;
- 22 E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;
- 23 F. For prejudgment interest on all amounts awarded; and
- 24
- 25
- 26
- 27
- 28

1 **G.** Such other and further relief as this Court may deem just and proper.

2 **DEMAND FOR JURY TRIAL**

3 Plaintiff hereby demands that this matter be tried before a jury.

4 DATE: October 25, 2023

5 **TOUSLEY BRAIN STEPHENS PLLC**

6 By: s/ Kim D. Stephens, P.S.
Kim D. Stephens, P.S., WSBA #11984

7 By: s/ Rebecca L. Solomon
Rebecca L. Solomon, WSBA #51520
1200 Fifth Avenue, Suite 1700
8 Seattle, WA 98101
Telephone: (206) 682-5600
9 Facsimile: (206) 682-2992
10 kstephens@tousley.com
rsolomon@tousley.com

11 Gary M. Klinger*
12 **MILBERG COLEMAN BRYSON PHILLIPS**
13 **GROSSMAN, PLLC**
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
14 Telephone: (866) 252-0878
gklinger@milberg.com

15 Glen L. Abramson*
16 Alexandra M. Honeycutt*
17 **MILBERG COLEMAN BRYSON PHILLIPS**
18 **GROSSMAN, PLLC**
800 S. Gay Street, Suite 1100
Knoxville, TN 37929
19 Telephone: (866) 252-0878
gabramson@milberg.com
20 ahoneycutt@milberg.com

21 *Counsel for Plaintiff and the Putative Class*

22 * *pro hac vice* forthcoming